KPMG Cyber Threat Intelligence Platform

ViperSoftX – Targeting Password Managers & Cryptos

Kimsuky APT (aka. STOLEN PENCIL, Thallium, APT 43, ARCHIPELAGO and Black Banshee), is a North Korean threat group, that has been active since 2012. Kimsuky focuses on stealing geo-political information related to foreign policy, national security, nuclear policy & sanctions that are of interest to the North Korean regime. The group has evolved to use updated variants of tools in their existing arsenal to target specific individuals as part of their ongoing cyber espionage campaigns. Their targets include government organizations, DPRK-defector support organizations, research centers & universities across US, South Korea, Europe, and Asia.

ViperSoftX distributes itself by leveraging illegal software packages like cracks, activators, etc., obtained from illicit websites & torrents. The malware unfolds as a multi-stage attack, with its initial payload concealed within a carrier software alongside a decryptor/loader DLL, which decrypts and executes the payload as admin. On execution, the malware performs anti-VM checks using WQL commands & virtualization strings before executing PowerShell code to download the main routine. To ensure persistence it drops a script under %APPDATA% folder bearing a legitimate name & adds its shortcut to the startup folder. Further, it connects with C2 to fetch commands for execution, implementing a 3-second sleep after each execution. Employs evasion techniques like byte mapping encryption, DLL side loading and disables web browser communications to C2 & changes C2 servers monthly to hinder analysis. Further, it executes man-in-the-browser attacks to steal cryptocurrency via API request tampering and installs malicious extensions. Additionally, it downloads scripts to crawl for crypto wallets & password managers like KeePass2 & 1Password for exploiting known vulnerabilities.

Gauging from the level of sophistication of the techniques employed by ViperSoftX, its evident that threat actors are evolving to execute a seamless chain of malware execution while becoming hard to detect.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/TAXII/MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

ViperSoftX – Targeting Password Managers & Cryptos

Indicators of Compromise: IP Addresses	
45.58.52[.]82	108.62.141[.]33
23.106.122[.]16	173.234.155[.]126
216.189.154[.]6	173.205.125[.]124

Indicators of Compromise: Domains	
mc.pzs[.]kr	kr-me[.]click
gdtech[.]kr	rfa[.]ink
siekis[.]com	smtper[.]org
ddim.co[.]kr	jp-ssl[.]work
kr-me[.]click	riaver[.]site
db-online[.]space	csnaver[.]com
com-view[.]online	naverdns[.]co
com-price[.]space	ssltop[.]work
lowerp.onlinewebshop[.]net	dubai-1[.]com
zetaros.000webhostapp[.]com	msdatl3[.]inc

Indicators of Compromise: Hashes
e2f05f91a56c5e9936e06d2e62f49b2c
c48221dba16382aeff0ac35aa0b93682
b13e7af2e9e964f16853d6fb2b38a8a0
9f8d0510cadccc2d123aea6a52684d28
01e971c39e6f9e199d5e9d5a595dd2cf
000130a373ea4085b87b97a0c7000c86
6b2062e61bcb46ce5ff19b329ce31b03
012d5ffe697e33d81b9e7447f4aa338b
582a033da897c967faade386ac30f604
51527624e7921a8157f820eb0ca78e29
04bb7e1a0b4f830ed7d1377a394bc717
582a033da897c967faade386ac30f604
012d5ffe697e33d81b9e7447f4aa338b
89c0e93813d3549efe7274a0b9597f6f

KPMG

KPMG Cyber Threat Intelligence Platform

ViperSoftX – Targeting Password Managers & Cryptos

Indicators of Compromise: Hashes
96d29a2d554b36d6fb7373ae52765850c17b68df
912f875899dd989fbfd64b515060f271546ef94c
8f2e6719ce0f29c2c6dbabe5a7bda5906a99481c
84398dcd52348eec37738b27af9682a3a1a08492
49c70c292a634e822300c57305698b56c6275b1c
0288140be88bc3156b692db2516e38f1f2e3f494
d1836aa050ec09b5c86ce4c0e14e0115a6a6510a
371d2c65283178192fa982671f2418c007182f3f
76f3f377aa66f9beaa8a103a4dd67f4fdcbeaa0d
750cd6daa87fd87b5c5b60ae1054719248274a9e
502930a3699ab8f638503fac656c1e180938ed3a
c3e97c29a2c64e823c447ac3a88219af70026576
15d9903e7d475d6927e0687ca238642678c90d2f
5f5432a5f992d8564c4db9074aaca1acb32a4687
3cb7e6aaef18bda503695deffc6154c4131c4988
13062d3e7da6b6b05cea3391356fa6ea6d731dcb
c9d4eb66b4a150dc27f881b7a7b935f4253d1cfb
c0ee5199cc15ed05fc6edf62a193deb819572cee
39a61c4d9d25c8ed1b38b1a51a8ef0b5cf51ce10
3e621ef83f474ee62a840f10d4a3f5877d9ee09e
a7461e60ae7297c20e1af5f83c42e34da2602b91
6519616b2ea5d2295241dc60b1aabc0766339364
6a486084d9181d7e8ef00f60164b7aa6719eb146
326575e1df8e63ccc3f8283c6bf01b186dac7088
03c35e4c6a641373db665e7d58cea421188fbc82
4db3f34d439e3d7a04df74e109012da671495c08
9944ce9354fb8961826339770ffc118000058271
de700699e8185497a82bb121fcc4cc6b470f1ce3
9eed1a4a84bcf2462a6556f62abb78e1c6386eba
287fd7e08214d4875c817f997714cf6510a57717
1baf12a0187261b79c263cb3b42c68b24ef3ca9d
ee4a54acd541dae48487514bde8730f491f125f5d6a50896b63a7ed04382c49c
e60ee5a5a4cad681ece20ae31d0b060ca73ea8ea034b2f23089f3b80db07133f
bbcfcc719190f0a2c687778d5d2fd5c6e345d64f44a01b26d33b7df20e099d6f

KPMG

KPMG Cyber Threat Intelligence Platform

ViperSoftX – Targeting Password Managers & Cryptos

Indicators of Compromise: Hashes
8c14dd8147c3c333e6f99d7f27a16203b4392abeeb51f5e56820ae0ee98f4a94
0c723ee38c21fdfffb3fdfac20d179d9e5bd3b4dadb6f0b4c847a140909cf95c
29e17b37a49218c644b8c7dcd981716be8c561704eab98f829cd1b97bb9e6f4d
1334ef6ae02e3d0581f3ac177aec7660628e26f764ee7064d3758fc4a34e8475
2c20ac485fd55bd1a5c4b75c5ba521e5b19912325737617178dfcb5a4e408aef
7a45a529b275cfaa6ebde88bf00413a11c0f701bf9e1e7e93ef27423fd17e3f5
031bde16d3b75083b0adda754aa982d4f6bd91e6b9d0531d5486dc139a90ce5a
539231dea156e29bd6f7ed8430bd08a4e07ba330a9fad799fea45d9e9eed070c
fdd0e18e841d3ec4e501dd8bf0da68201779fd90237c1c67078d1d915cd13045
a4daa30a2ef6943d8eec7759246f6584bfd679b094cb8b66302355500a036b9a
11b99f460bf14c902083d2c9559da6f65ab376bcde5c63919a569ad5b5812d3d
21f1bd334198763e3fd43b3f466989549d306c490e2f1d6a92df2c5810b65cb8
a2e6e833947a1d5c526c0c2d6943e35bad9cbe22b52a6f7013ab8c1de0aa2d31
486b279a9988871c329e2bbe14328f321818cc5f8e878900366ca1051afa7ea9
db18e23bebb8581ba5670201cea98ccf71ecea70d64856b96c56c63c61b91bbe
7903bdf0976d5c6f3c28abf40c41414380f4494a8bf72af9e27ff810599faaf2
6a435e2aab6dce39d626eacb39fc964967e35e94abf513da0f6511ab7b1f826e